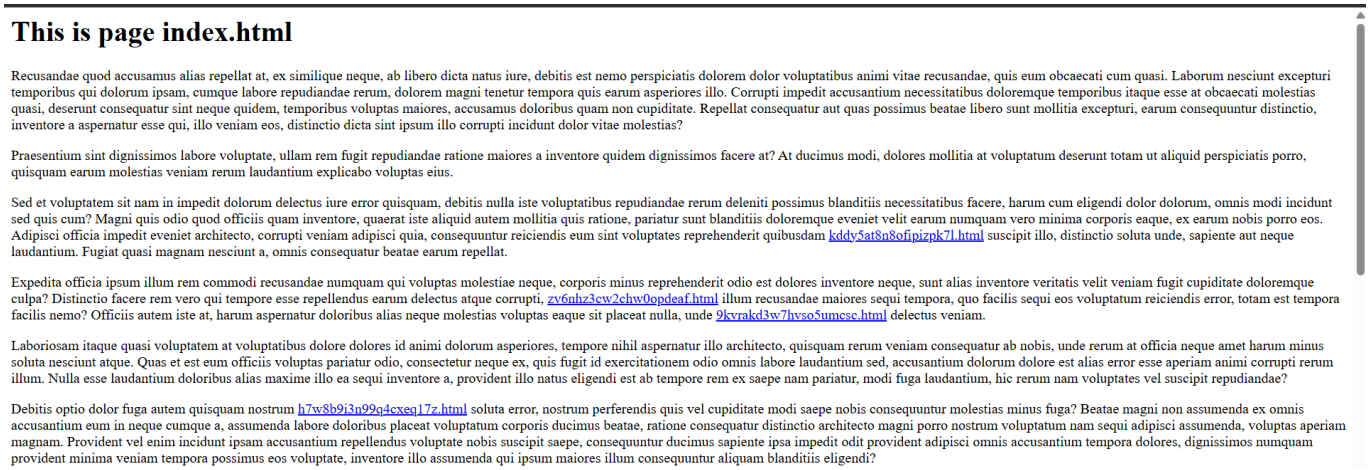
Web - DeepWeb - 75 points

Kévin DUVERGER

Table des matières

1 Résolution DeepWeb :

Tentons une nouvelle fois de nous connecter au serveur web (sur `http://146.59.227.136:23417`) :



This is page index.html

Recusandae quod accusamus alias repellat at, ex similique neque, ab libero dicta natus iure, debitis est nemo perspiciatis dolorem dolor voluptatibus animi vitae recusandae, quis eum obcaecati cum quasi. Laborum nesciunt excepturi temporibus qui dolorum ipsam, cumque labore repudiandae rerum, dolorem magni tenetur tempora quis earum asperiores illo. Corrupti impedit accusantium necessitatibus doloremque temporibus itaque esse at obcaecati molestias quasi, deserunt consequatur sint neque quidem, temporibus voluptas maiores, accusamus doloribus quam non cupiditate. Repellat consequatur aut quas possimus beatae libero sunt mollitia excepturi, earum consequuntur distinctio, inventore a aspernatur esse qui, illo veniam eos, distinctio dicta sint ipsum illo corrupti incidunt dolor vitae molestias?

Praesentium sint dignissimos labore voluptate, ullam rem fugit repudiandae ratione maiores a inventore quidem dignissimos facere at? At ducimus modi, dolores mollitia at voluptatum deserunt totam ut aliquid perspiciatis porro, quisquam earum molestias veniam rerum laudantium explicabo voluptas eius.

Sed et voluptatem sit nam in impedit dolorum delectus iure error quisquam, debitis nulla iste voluptatibus repudiandae rerum deleniti possimus blanditiis necessitatibus facere, harum cum eligendi dolor dolorum, omnis modi incidunt sed quis cum? Magni quis odio quod officiis quam inventore, quaerat iste aliquid autem mollitia quis ratione, pariatur sunt blanditiis doloremque eveniet velit earum numquam vero minima corporis eaque, ex earum nobis porro eos. Adipisci officia impedit eveniet architecto, corrupti veniam adipisci quia, consequuntur reiciendis eum sint voluptates reprehenderit quibusdam kddy5at8n8ofipizpk7l.html suscipit illo, distinctio soluta unde, sapiente aut neque laudantium. Fugiat quasi magnam nesciunt a, omnis consequatur beatae earum repellat.

Expedita officia ipsum illum rem commodi recusandae numquam qui voluptas molestiae neque, corporis minus reprehenderit odio est dolores inventore neque, sunt alias inventore veritatis velit veniam fugit cupiditate doloremque culpa? Distinctio facere rem vero qui tempore esse repellendus earum delectus atque corrupti, zv6nhz3cw2chw0opdeaf.html illum recusandae maiores sequi tempora, quo facilis sequi eos voluptatum reiciendis error, totam est tempora facilis nemo? Officiis autem iste at, harum aspernatur doloribus alias neque molestias voluptas eaque sit placeat nulla, unde 9kvrakd3w7hvso5umcsc.html delectus veniam.

Laboriosam itaque quasi voluptatem at voluptatibus dolore dolores id animi dolorum asperiores, tempore nihil aspernatur illo architecto, quisquam rerum veniam consequatur ab nobis, unde rerum at officia neque amet harum minus soluta nesciunt atque. Quas et est eum officiis voluptas pariatur odio, consectetur neque ex, quis fugit id exercitationem odio omnis labore laudantium sed, accusantium dolorum dolore est alias error esse aperiam animi corrupti rerum illum. Nulla esse laudantium doloribus alias maxime illo ea sequi inventore a, provident illo natus eligendi est ab tempore rem ex saepe nam pariatur, modi fuga laudantium, hic rerum nam voluptates vel suscipit repudiandae?

Debitis optio dolor fuga autem quisquam nostrum h7w8b9i3n99q4cxeq17z.html soluta error, nostrum perferendis quis vel cupiditate modi saepe nobis consequuntur molestias minus fuga? Beatae magni non assumenda ex omnis accusantium eum in neque cumque a, assumenda labore doloribus placeat voluptatum corporis ducimus beatae, ratione consequatur distinctio architecto magni porro nostrum voluptatum nam sequi adipisci assumenda, voluptas aperiam magnam. Provident vel enim incidunt ipsam accusantium repellendus voluptate nobis suscipit saepe, consequuntur ducimus sapiente ipsa impedit odit provident adipisci omnis accusantium tempora dolores, dignissimos numquam provident minima veniam tempora possimus eos voluptate, inventore illo assumenda qui ipsum maiores illum consequuntur aliquam blanditiis eligendi?

Vous voyez que l'on peut trouver nombreux liens vers d'autres pages.

On peut récupérer la liste des liens dans cette première page avec le script suivant :

```
chaineFinale = "";
elements = document.getElementsByTagName("a")
for (i = 0; i < elements.length; i++) {
    chaineFinale += elements[i].href + "\n";
}
console.log(chaineFinale);
```

Et voici la-dite liste :

```
http://146.59.227.136:23417/kddy5at8n8ofipizpk7l.html
http://146.59.227.136:23417/zv6nhz3cw2chw0opdeaf.html
http://146.59.227.136:23417/9kvrakd3w7hvso5umcsc.html
http://146.59.227.136:23417/h7w8b9i3n99q4cxeq17z.html
http://146.59.227.136:23417/dnvaevgxiv5aw38jg4gp.html
http://146.59.227.136:23417/66eyu9dzd7gb09z5vrzl.html
http://146.59.227.136:23417/dj088932w7qw8velggxt.html
http://146.59.227.136:23417/61lmlvcn9q99cezrxkdv.html
http://146.59.227.136:23417/k5wyavfyroy8xhk83620.html
http://146.59.227.136:23417/333qzrxfjxtko91zug2w.html
```

On peut donc tenter de récupérer toutes les pages du site web et peut être qu'une contient le flag. Il faudra également bien faire attention aux pages dupliquées. Voici le code qui arrive à faire cela :

```
import requests

# Some initialisation
pagesSeen  = []
pagesToSee = [ "index.html" ]

# The loop
iteration = 0
while len(pagesToSee) > 0 :
    if pagesToSee[0] in pagesSeen :
        pagesToSee = pagesToSee[1:]
        continue
    iteration += 1
    print("Getting page number " + str(iteration) + " : " + str(pagesToSee[0]))
    # Getting content
    response = requests.get("http://146.59.227.136:23417/" + pagesToSee[0])
    if response.status_code != 200 :
        pagesToSee = pagesToSee[1:]
        continue
    # Now, we can analyze it (by getting all of the next pages)
    content = response.text
    indexInContent = 0
    while True :
        newIndex = content[indexInContent:].find("href=\"") + indexInContent
        if newIndex == indexInContent - 1 : break
        otherIndex = content[newIndex+6:].find("\"") + newIndex + 6
        newPage = content[newIndex+6:otherIndex].replace("http://146.59.227.136:23417/", "")
        if newPage not in pagesSeen :
```

```
            pagesToSee.append(newPage)
        indexInContent = otherIndex
    # Testing if "cryptis" is inside
    if "cryptisCTF{" in content :
        index = content.find("cryptisCTF{")
        print(content[index:index+50])
        break
    # Removing the first page to see
    pagesSeen.append(pagesToSee[0])
    pagesToSee = pagesToSee[1:]
```

Après cela, vous devriez obtenir la page qui contient le flag : `zbk858ddn6fwis8un5a9.html` !